



CVE-2003-0127

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2003-0127
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-03-31 05:00:00 UTC
Updated	2018-05-03 01:29:00 UTC
Description	The kernel module loader in Linux kernel 2.2.x before 2.2.25, and 2.4.x before 2.4.21, allows local users to gain root privileges.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.2.0	All	All	All
Operating System	Linux	Linux Kernel	2.2.1	All	All	All
Operating System	Linux	Linux Kernel	2.2.10	All	All	All
Operating System	Linux	Linux Kernel	2.2.11	All	All	All
Operating System	Linux	Linux Kernel	2.2.12	All	All	All
Operating System	Linux	Linux Kernel	2.2.13	All	All	All
Operating System	Linux	Linux Kernel	2.2.14	All	All	All
Operating System	Linux	Linux Kernel	2.2.15	All	All	All
Operating System	Linux	Linux Kernel	2.2.16	All	All	All
Operating System	Linux	Linux Kernel	2.2.17	All	All	All
Operating System	Linux	Linux Kernel	2.2.18	All	All	All
Operating System	Linux	Linux Kernel	2.2.19	All	All	All
Operating System	Linux	Linux Kernel	2.2.2	All	All	All
Operating System	Linux	Linux Kernel	2.2.20	All	All	All
Operating System	Linux	Linux Kernel	2.2.21	All	All	All
Operating System	Linux	Linux Kernel	2.2.22	All	All	All
Operating System	Linux	Linux Kernel	2.2.23	All	All	All

Operating System	Linux	Linux Kernel	2.2.24	All	All	All
Operating System	Linux	Linux Kernel	2.2.3	All	All	All
Operating System	Linux	Linux Kernel	2.2.4	All	All	All
Operating System	Linux	Linux Kernel	2.2.5	All	All	All
Operating System	Linux	Linux Kernel	2.2.6	All	All	All
Operating System	Linux	Linux Kernel	2.2.7	All	All	All
Operating System	Linux	Linux Kernel	2.2.8	All	All	All
Operating System	Linux	Linux Kernel	2.2.9	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All
Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.20	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
Operating System	Linux	Linux Kernel	2.2.0	All	All	All
Operating System	Linux	Linux Kernel	2.2.1	All	All	All
Operating System	Linux	Linux Kernel	2.2.10	All	All	All
Operating System	Linux	Linux Kernel	2.2.11	All	All	All
Operating System	Linux	Linux Kernel	2.2.12	All	All	All

Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All

References						
Reference	Source		Link	Tags		
Debian -- Security Information -- DSA-423-1 linux-kernel-2.4.17-ia64	DEBIAN		www.debian.org			
Gentoo Linux — Error 404 (Not Found)	GENTOO		security.gentoo.org			
Debian -- Security Information -- DSA-332-1 linux-kernel-2.4.17	DEBIAN		www.debian.org			
redhat.com Red Hat Support	REDHAT		rhn.redhat.com	Patch, V		
redhat.com Red Hat Support	REDHAT		www.redhat.com			
Debian -- Security Information -- DSA-276-1 linux-kernel-s390	DEBIAN		www.debian.org			
'[ESA-20030515-017] 'kernel' several bug and security-related fixes.' - MARC	ENGARDE		marc.info			
Debian -- Security Information -- DSA-495-1 linux-kernel-2.4.16-arm	DEBIAN		www.debian.org			
Debian -- Security Information -- DSA-312-1 kernel-patch-2.4.18-powerpc	DEBIAN		www.debian.org			
CSSA-2003-020.0	CALDERA		ftp.caldera.com			
redhat.com Red Hat Support	REDHAT		rhn.redhat.com			
US-CERT Vulnerability Note VU#628849	CERT-VN		www.kb.cert.org	Third Pa		
Debian -- Security Information -- DSA-311-1 linux-kernel-2.4.18	DEBIAN		www.debian.org			
Debian -- Security Information -- DSA-270-1 linux-kernel-mips	DEBIAN		www.debian.org			
Repository / Oval Repository	OVAL		oval.cisecurity.org			
Support	REDHAT		www.redhat.com			
Neohapsis Archives - VulnWatch - #0134 - [VulnWatch] Fwd: Ptrace hole / Linux 2.2.25	VULNWATCH		archives.neohapsis.com			
Debian -- Security Information -- DSA-336-1 linux-kernel-2.2.20	DEBIAN		www.debian.org			
Advisories - Mandriva	MANDRAKE		www.mandriva.com			
Advisories - Mandriva	MANDRAKE		www.mandriva.com			
CVE Program record	CVE.ORG		www.cve.org	canonic		
NVD vulnerability detail	NVD		nvd.nist.gov	canonic		

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)